BARNES & THORNBURG LLP

# Regulation S-P Violation: Are You Prepared For A Cyber-Security Breach?

October 8, 2015 | | SEC,The GEE Blog

**Trace Schmeltz**
Partner
Financial and Regulatory Litigation Group
Co-Chair, Fintech Co-Chair

On Sept. 22, 2015, the Securities and Exchange Commission (SEC) announced the first violation by a registered investment advisor of the so-called Safeguards Rule (Regulation S-P) pertaining to the protection of personally identifiable information from cyber-attack. This is the first instance of the SEC enforcing Regulation S-P against an investment advisor. The Regulation, broadly speaking, requires broker-dealers, investment advisers and other financial firms to protect confidential customer information from unauthorized release to unaffiliated third parties. Included in Regulation S-P is the "Safeguard Rule" (Rule 30(a)), which requires financial institutions to, among other things, adopt written policies and procedures reasonably designed to protect customer information against cyber-attacks. This raises the question: Are you prepared for a cyber-attack (and the attendant liability)? In its findings, the SEC found that the registered investment advisor had stored personally identifiable information on a third-party server that was hacked. Ultimately, it appeared that the cyber-attack had come from China. It does not, at this time, appear that any of the personally identifiable information has been used. Furthermore, the registered investment advisor acted quickly to alert its clients about the attack and provided identity theft monitoring. Nonetheless, the SEC imposed a $75,000 fine on the registered investment advisor. Its primary reason for doing so was because the firm did not have sufficient written policies and procedures in place to protect personally identifiable information. It had, for example, allegedly failed to conduct periodic risk assessments, implement a firewall, or otherwise protect files from a cyber-attack. Ultimately, to be prepared for the same sort of investigation, a best practice for every registered investment advisor is to do a critical assessment of the manner in which its customer data is stored. Anticipate regulators requiring such data to be encrypted and otherwise secured from cyber-attack. For registered investment advisors using third-party service providers, a best practice is to ensure that the third-party service providers are audited and certified as having secure methods in place to protect customer personally identifiable information. In addition, registered investment advisors would be wise to ensure that they have some form of insurance coverage for those risks, including an investigation, fines and damages. Coverage for such regulatory investigations may be available under stand-alone cyberinsurance policies or in the form of coverage for regulatory investigations and actions under a director and officer liability

## RELATED PRACTICE AREAS

Financial and Regulatory Litigation
Government Litigation
Securities and Capital Markets
White Collar and Investigations

insurance policy. Cyberinsurance policies differ significantly in the market place, and the availability of regulatory investigation coverage under D&O insurance policies varies.  Registered investment advisors should consider consulting insurance coverage counsel to evaluate whether their insurance policies might provide insurance coverage for such matters.